IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

MARGUERITE KUROWSKI and BRENDA MCCLENDON, on behalf of themselves and all others similarly situated,	)	
Plaintiffs,	)	
vs.	)	**Case No. 22 C 5380**
RUSH SYSTEM FOR HEALTH d/b/a RUSH UNIVERSITY SYSTEM FOR HEALTH,	)	
Defendant.	)	

MEMORANDUM OPINION AND ORDER

MATTHEW F. KENNELLY, District Judge:

Marguerite Kurowski and Brenda McClendon (collectively Kurowski) filed suit in September 2022 against Rush University System for Health. Kurowski alleges that Rush has violated her and other patients' privacy interests by using tracking tools on its website that surreptitiously intercept and transmit to third parties information that includes patients' personally identifiable health data. Before the Court is Rush's motion for judgment on the pleadings under Federal Rule of Civil Procedure 12(c). For the following reasons, the Court grants the motion with respect to Kurowski's breach of contract claim but otherwise denies the motion.

Background

The Court has issued three previous decisions in this case: two decisions on motions to dismiss filed by Rush and one decision granting Kurowski's motion for leave

to file a second amended complaint. *See Kurowski v. Rush Sys. for Health*, 659 F. Supp. 3d 931 (N.D. Ill. 2023) (*Kurowski I*); *Kurowski v. Rush Sys. for Health*, 683 F. Supp. 3d 836 (N.D. Ill. 2023) (*Kurowski II*); *Kurowski v. Rush Sys. for Health*, No. 22 C 5380, 2023 WL 8544084 (N.D. Ill. Dec. 11, 2023) (*Kurowski III*). The Court assumes familiarity with the factual and procedural background of the case discussed in the previous orders and therefore provides only a brief summary. Kurowski is a Rush patient who uses Rush's website and its online patient portal, MyChart, to communicate with her healthcare providers about appointments, test results, prescription refills, and other treatment.

Kurowski alleges that Rush programmed its website and its MyChart system to secretly deploy tracking technology from Google, Facebook, and Bidtellect that allows for contemporaneous and unauthorized interception and transmission of the patients' interactions with Rush's website and MyChart, including "the precise content of patient communications with Rush." Second Am. Compl. ¶ 32. This includes, for example, the name and location of a patient's personal physician, the physician's specialty, and the patient's conditions. The tracking technology also collects a wealth of data that Google, Facebook, and Bidtellect use to identify the patient and show them targeted advertising. The data collected includes patient IP addresses, patient cookie identifiers, device identifiers, account numbers, URLs, other unique identifying numbers or codes, and browser fingerprints.

The operative second amended complaint includes three claims. First, Kurowski alleges that that Rush violated the federal Wiretap Act (count one). Second, she alleges that Rush breached its contract with her (count two). Third, she alleges that

Rush violated the Illinois Eavesdropping Act (count three).

Discussion

Federal Rule of Civil Procedure 12(c) states that "[a]fter the pleadings are close—but early enough not to delay trial—a party may move for judgment on the pleadings." In deciding a Rule 12(c) motion, the Court "employ[s] the same standard that applies when reviewing a motion to dismiss for failure to state a claim under Rule 12(b)(6)." *Buchanan-Moore v. County of Milwaukee*, 570 F.3d 824, 827 (7th Cir. 2009). "To survive a motion for judgment on the pleadings (or a motion to dismiss), the complaint must 'state a claim to relief that is plausible on its face.'" *ADM All. Nutrition, Inc. v. SGA Pharm Lab, Inc.*, 877 F.3d 742, 746 (7th Cir. 2017) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). At this stage, the Court must "accept all well-pleaded facts in the complaint as true and draw all reasonable inferences in the plaintiff's favor." *NewSpin Sports, LLC v. Arrow Elecs., Inc.*, 910 F.3d 293, 299 (7th Cir. 2018).

A. Wiretap Act claim

Under the Wiretap Act, any person who "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication" commits an offense and may be subject to a civil penalty. 18 U.S.C. §§ 2511(1), (4) & (5). This is also true for any person who intentionally discloses or uses, or endeavors to disclose or use, the contents of an intercepted communication. *Id.* § 2511(1)(c), (d). The statute provides an exception if the person intercepting or causing an interception of a communication "is a party to the communication." *Id.* § 2511(2)(d). But this "party exception" does not apply if the

"communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State." *Id.*

The Court previously concluded that Rush was a "party" to the intercepted communications for purposes of the party exception. *See Kurowski I*, 659 F. Supp. 3d at 938. Kurowski argued that the crime-or-tort exception to the party exception nevertheless subjected Rush to liability under the Wiretap Act because she alleged that Rush acted with the purpose of making unauthorized disclosures of patient health data in violation of the Health Insurance Portability and Accountability Act (HIPAA). Specifically, Kurowski argued that Rush had violated HIPAA by "knowingly . . . disclos[ing] individually identifiable health information" (IIHI) to a third party without authorization. 42 U.S.C. § 1320d-6(a)(3).

In *Kurowski I* and *II*, the Court disagreed with this argument because Kurowski had not "alleged sufficient facts . . . to support an inference that Rush disclosed its patients' individually identifiable health information, at least as that term is defined by the statute." *Kurowski I*, 659 F. Supp. 3d at 938. The statutory definition of IIHI is

> any information, including demographic information collected from an individual, that—(A) is created or received by a health care provider ... and (B) *relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual*, and—(i) identifies the individual; or (ii) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

42 U.S.C. § 1320d(6) (emphasis added). The Court concluded that, because the first two versions of Kurowski's complaint alleged only that the tracking tools collected IP addresses, cookie identifiers, device identifiers, account numbers, URLs, and browser fingerprints, the allegations were "far too vague to allow an inference to be drawn that

Rush was actually disclosing IIHI as it is unambiguously defined by HIPAA, rather than just metadata." *Kurowski II*, 683 F. Supp. 3d at 843. The Court noted that, although "the actual *substance* of Kurowski's *private* communications *related to her care* . . . would likely fall under section 1320d(6)'s definition of IIHI," Kurowski had "failed to plausibly allege that anything of that nature was actually disclosed." *Id.* at 844.

Kurowski then moved for leave to file a second amended complaint. The Court concluded that she had added new factual allegations to support her claim that Rush had collected IIHI as defined by HIPAA. *See Kurowski III*, 2023 WL 8544084, at *3. "In particular, Kurowski (again, a term used to reference the two plaintiffs collectively) alleges that Rush . . . transmitted the name and location of her personal physician, as well as her physician's specialty" to Facebook, Google, and Bidtellect, and that this information was used "to target her with particular advertising associated with her particular health conditions." *Id.* With the additional facts, the Court concluded, the complaint sufficiently alleged that Rush was intercepting and transmitting IIHI and not merely metadata. The Court further concluded that Kurowski had sufficiently alleged "that Rush knowingly transmits this data and that it does so for the purpose of financial gain." *Id.* The Court granted leave to file a second amended complaint because these allegations, taken together, were sufficient to invoke the crime-or-tort exception premised on Rush's violation of HIPAA and thus to state a claim for relief under the Wiretap Act.

Rush does not dispute, for purposes of its motion for judgment on the pleadings, the Court's conclusion that Kurowski has stated a plausible HIPAA violation. But Rush argues that the Court erred in concluding that her allegations were sufficient to invoke

the crime-or-tort exception. Specifically, Rush emphasizes that the crime-or-tort exception does not apply "merely because Rush allegedly violated the law." Def's. Mot. for J. on the Pleadings at 4. Instead, the exception requires that Rush acted "for the *purpose* of committing any criminal or tortious act." 18 U.S.C. § 2511(2)(d) (emphasis added). In Rush's view, this "purpose" requirement precludes application of the crime-or-tort exception to its conduct because it was not on notice that its conduct violated HIPAA: "How could Rush have in mind a purpose to criminally violate HIPAA *at the time the alleged disclosures were made* when, *at this time*, plaintiffs have not plausibly alleged that Rush was even on notice that the statute applied to the alleged internet disclosures at issue?" Def.'s Mot. for J. on the Pleadings at 6. In support of its argument, Rush argues that the Department of Health and Human Services did not issue a bulletin alerting HIPAA-regulated entities that using online tracking tools like the ones in this case could violate the statute until December 2022, after this case was filed. Rush further argues that caselaw at the time of its violations suggested that its use of this technology did not violate HIPAA.

Kurowski responds that it does not matter whether Rush intended or believed it was violating HIPAA; rather, the relevant question is whether Rush "used the tracking technology at issue *knowingly, and for the purpose of, disclosing patient individually identifiable health information* for commercial or personal gain—a crime." Pls.' Resp. at 6. Kurowski also argues that Rush *did* know that its conduct violated HIPAA and therefore the crime-or-tort exception applies even under the more demanding standard proposed by Rush.

It appears that Rush raises two related questions about the crime-or-tort

exception. The first question is whether the section 2511(2)(d) requirement that a party act "for the purpose of committing any criminal or tortious act" requires the party to know that the criminal or tortious act it seeks to commit is, in fact, against the law. The second question is whether Kurowski has sufficiently alleged that Rush acted "for the purpose of" making unauthorized disclosures of her IIHI rather than merely with the knowledge that it was making such disclosures.

1. Knowledge of illegality

Rush interprets the "purpose" requirement of the crime-or-tort exception as requiring a party to have knowledge that its intended use of the intercepted information is illegal. Although the "general rule" is that "ignorance of the law or a mistake of law is no defense," it is well established that some statutes require, as an element of the offense, the defendant to act with knowledge that it is breaking the law. *Cheek v. United States*, 498 U.S. 192, 200 (1991). The Supreme Court has explained that, in the criminal context, Congress's use of the term "willfully" can in some circumstances "carv[e] out an exception to the traditional rule" and require "a voluntary, intentional violation of a known legal duty." *Id.*; *see also Bryan v. United States*, 524 U.S. 184, 191–92 (1998) ("As a general matter . . . in order to establish a 'willful' violation of a statute, 'the government must prove that the defendant acted with knowledge that his conduct was unlawful.'" (quoting *Ratzlaf v. United States*, 510 U.S. 135, 137 (1994))). This kind of willfulness requirement is most commonly present in criminal offenses based on highly technical areas of the law, such as certain tax offenses. *See Cheek*, 498 U.S. at 201 ("This special treatment of criminal tax offenses is largely due to the complexity of the tax laws.").

Although Rush does not discuss this line of cases, it appears to assume that the "purpose" requirement of the crime-or-tort exception superimposes this type of willfulness requirement on top of the mens rea required for the underlying crime or tort. Kurowski, in contrast, argues that the purpose requirement does not require Rush to have believed that its conduct violated the law; rather, it requires only that Rush's intended to use the intercepted communications in a manner proscribed by law.

The Seventh Circuit has not directly addressed this question. Rush points the Court to *Desnick v. American Broadcasting Companies, Inc.*, 44 F.3d 1345 (7th Cir. 1995). In *Desnick*, the defendant television network, ABC, sent undercover "testers" with secret cameras to pose as patients to the plaintiffs' ophthalmic clinic. *Id.* at 1347–48. ABC later used the footage in a program in which it claimed the plaintiffs were committing Medicare fraud by recommending and conducting unnecessary cataract surgery on Medicare recipients. *Id.* The plaintiffs filed suit against ABC alleging, among other claims, that it had violated the Wiretap Act. Because the testers were "party" to the conversations, whether the plaintiffs stated a claim turned on the crime-or-tort exception. The Seventh Circuit concluded that, even if "the program as it was eventually broadcast was [defamatory]," the crime-or-tort exception did not apply because "there [was] no suggestion that the defendants sent the testers into the [plaintiffs'] offices for the purpose of defaming the plaintiffs . . . ." *Id.* at 1353.

The Court reads *Desnick* as standing for the proposition that the crime-or-tort exception requires a court to look to the party's intentions at the time it committed the alleged Wiretap Act violation—more specifically, whether it intended at that point to commit a tort or crime—not whether the party later misused an intercepted

communication in furtherance of a separate crime. But *Desnick* does not say, or suggest that the defendant must know that the criminal or tortious act it is committing is, in fact, a crime or tort.

The Court sees no persuasive reason to read a heightened willfulness requirement into the crime-or-tort exception. As the Court has discussed, courts generally interpret statutes as imposing knowledge-of-the-law requirements in cases involving "highly technical statutes that present[ ] the danger of ensnaring individuals engaged in apparently innocent conduct." *Bryan*, 524 U.S. at 194. But the "purpose" requirement of the statutory provision at issue here, section 2511(2)(d), applies to "any criminal or tortious act in violation of the Constitution or laws of the United States or of any State." That sweeps in both sophisticated offenses and straightforward ones. Moreover, the Court sees no reason to presume that the mens rea requirements of the underlying torts or crimes do not already address concerns about separating innocent from criminal or tortious conduct. In this case, for example, the underlying HIPAA provision, section 1320d-6(a)(3), requires that Rush acted "knowingly"—a requirement the Court has already found satisfied at the pleading stage and that Rush does "not re-argue" in its motion for judgment under Rule 12(c). Def.'s Mot. for J. on the Pleadings at 1. The Court thus concludes that the phrase "for the purpose of" does not require that a party act with knowledge that its intended use of the intercepted communication is illegal.

2. "Purpose" versus "knowledge"

This conclusion does not mean, however, that the "purpose" requirement adds nothing to the equation. "Purpose and knowledge are the most culpable levels in the

criminal law's mental-state 'hierarchy.'" *Borden v. United States*, 593 U.S. 420, 426 (2021) (quoting *United States v. Bailey*, 444 U.S. 394, 404 (1980)). The Supreme Court has explained that the distinction between acting with purpose and acting with knowledge is often "limited," "narrow," and "inconsequential." *Id.* Generally, however, "[a] person acts purposefully when he 'consciously desires' a particular result." *Id.* (quoting *Bailey*, 444 U.S. at 404). In contrast, a person acts "knowingly when 'he is aware that [a] result is practically certain to follow from his conduct,' whatever his affirmative desire." *Id.* (quoting *Bailey*, 444 U.S. at 404).

The Court concludes that Kurowski has plausibly alleged that Rush acted with the "conscious desire" to "knowingly . . . disclose[ ] individually identifiable health information" to a third party without authorization when it employed the tracking technology at issue in its web properties. 42 U.S.C. § 1320d-6(a)(3). First, Kurowski alleges in her complaint that Rush had at least some degree of control over what information would or would not be intercepted and transmitted by the tracking technologies. Taking these allegations as true (as required at this stage of the case), it appears that Rush had the ability to select *which* specific pages within its web properties would intercept and transmit patients' communications to Facebook, Google, and Bidtellect, and that it actively chose to employ the tracking technology on certain pages of its website that were likely to contain IIHI, such as within the MyChart patient portal or on pages prompting patients to schedule appointments. *See* Second Am. Compl. ¶ 96 ("Rush deploys Google tracking tools on nearly every page on its web properties, including within the MyChart patient portal . . . ."). Kurowski also alleges, for example, that Rush chose *not* to take measures such as anonymizing patients' IP

addresses even when the tracking technology offered that option. *See id.* ¶¶ 94–95. A reasonable factfinder could infer from Rush's specific choices regarding how to employ the tracking technology that Rush "consciously desired" to intercept and transmit patients' IIHI.

Rush suggests that it did not act with the requisite purpose because it employed the tracking technologies at issue for a "financial motive," as some out-of-circuit district courts have held. *See, e.g.*, *In re DoubleClick Inc. Privacy Litig.*, 154 F. Supp. 2d 497, 519 (S.D.N.Y. 2001) ([The defendant's] purpose has plainly not been to perpetuate torts on millions of Internet users, but to make money by providing a valued service to commercial Web sites."). The Court disagrees. First, the Seventh Circuit has stated that the crime-or-tort exception turns on the defendant's "intended use" of the interception at the time it is intercepted, not on the defendant's "motive." *See In re High Fructose Corn Syrup Antitrust Litig.*, 216 F.3d 621, 626 (7th Cir. 2000) ("[W]hen the law speaks of recording conversations with a criminal or tortious purpose, it has, we think, regard for the intended use of the recordings," and thus the defendant's "*motive* in making the recordings" was not relevant to the analysis.). Many crimes and torts are motivated by a desire to make money, and "it defies common sense that a clearly harmful act could escape liability as long as it was done for profit." *Mekhail v. N. Mem'l Health Care*, No. 23 C 00440, 2024 WL 1332260, at *5 n.4 (D. Minn. Mar. 28, 2024). Second, nothing in section 2511(2)(d) requires that a party act with the *sole* purpose of committing the underlying crime or tort. Thus, even if the Court views Rush's "purpose" in employing the tracking technologies as, for example, improving its advertising outcomes and its profit margins, that does not mean that it didn't also "consciously

desire" to make unauthorized disclosures of Kurowski's IIHI to achieve that goal.

It is also worth noting that, by its plain language, the relevant HIPAA provision simply proscribes knowing disclosure of IHII; it doesn't require (or exclude) any particular motive. Courts don't generally add words to the language Congress chose, not even under the guise of interpretation. *See, e.g., Muldrow v. City of St. Louis*, 144 S. Ct. 967, 974 (2024); *Water Quality Ass'n Employees' Ben. Corp. v. United States*, 795 F.2d 1303, 1309 (7th Cir. 1986).

3. If required, Kurowski has sufficiently alleged knowledge of illegality

The Court further concludes that, even if it agreed with Rush that the crime-or-tort exception requires that Rush knew it was violating the law, Kurowski's allegations are sufficient to state a claim at the pleading stage.

Rush argues that it could not have known that "*at the time of the alleged disclosures in question* . . . that HIPAA even applied to the alleged transferences of internet information at issue." Def.'s Mot. for J. on the Pleadings at 1. Specifically, Rush argues that at the time of the alleged violations, "the only federal courts to weigh in on this issue had both held that HIPAA did not apply to the alleged disclosures at issue at all." *Id.* at 6. Rush first cites to this Court's dismissal of the first two versions of Kurowski's complaint. It is true that the Court twice dismissed Kurowski's Wiretap Act claim. But again, that was because she "alleged only that IP addresses, cookie identifiers, device identifiers, account numbers, URLs, and browser fingerprints were transmitted to third parties like Facebook, Google, and Bidtellect," and the Court found "no basis in the complaint to support a plausible inference that such information (at least without more) constituted IIHI within the meaning of HIPAA." *See Kurowski III*, 2023 WL

8544084, at *2. This case, however, is not about that information and nothing more. Rush disregards the fact that the Court granted Kurowski's motion to file a second amended complaint with respect to her Wiretap Act claim precisely because she included "additional factual allegations regarding the information she contends was transmitted to third parties with Rush's knowledge and at its instance" that made clear that she alleged that *her IIHI* was transmitted. *Id.* Kurowski alleged, for example, that the information included her status as a Rush patient and "patient communications pertaining to or about specific doctors, conditions, treatments, payments, and connections to the MyChart portal." *Id.* A reasonable factfinder could infer that a sophisticated healthcare provider would be aware that this kind of information is IIHI under HIPAA.

Rush next cites to *Smith v. Facebook, Inc.*, 262 F. Supp. 3d 943, 954 (N.D. Cal. 2017), *aff'd*, 745 F. App'x 8 (9th Cir. 2018), in which the district court held (and the Ninth Circuit affirmed) that the plaintiffs' IP address, cookies, browser information, and visits to websites containing "general health information that is accessible to the public at large" did not qualify as IIHI under HIPAA. But in contrast to the plaintiffs in *Smith*, Kurowski alleges that Rush intercepted and transmitted specific information regarding her appointments, providers, health conditions, and care as a Rush patient. This type of individualized patient data is not general, publicly accessible health information.

Rush also argues that the Department of Health and Human Services did not issue a bulletin warning that the use of the tracking technologies at issue in this case could violate HIPAA in December 2022, after this case was filed. *See* Dep't of Health & Hum. Servs., Use of Online Tracking Technologies by HIPAA Covered Entities and

Business Associates (Dec. 1, 2022) (HHS Bulletin). The Court disagrees. First, the Court expressly declined to defer to this bulletin in deciding whether Kurowski had stated a claim. To the contrary, as discussed, the Court agreed with Rush that its collection of only personally identifying "metadata" such as IP addresses, account identifiers, browser fingerprints, and so forth was not sufficient to plausibly allege that Rush knowingly disclosed IIHI. *See Kurowski II*, 683 F. Supp. 3d at 843. The Court permitted Kurowski to proceed with her Wiretap Act claim only when she added factual allegations that her private, care-related communications were also intercepted and transmitted in addition to the personally identifying information. Second, the Court disagrees with the proposition that a party cannot know that it is violating a law unless it has been specifically informed of that fact by a government agency. Third, as Kurowski points out, the HHS bulletin that Rush relies on states that "it has always been true that regulated entities may not impermissibly disclose [personal health information] to tracking technology vendors." Pl.'s Resp. at 5–6 (quoting HHS Bulletin). In brief, although Rush may argue that the bulletin supports its position that it did not know its use of tracking technologies violated HIPAA, it does not establish that it could not have known as a matter of law.

The Court recognizes that covered entities may face uncertainty regarding the outer limits of what HIPAA protects and whether they can ever use tracking technology on their websites without violating the statute. But Kurowski's allegations in the second amended complaint include information that would clearly constitute IIHI, such as Kurowski's communications with her provider, her medical conditions, her appointments, and so forth. As the Court previously explained, "private, care-related communications

fall squarely within the meaning of IIHI as contemplated by the statute." *Kurowski II*, 683 F. Supp. 3d at 843. The Court does not see how Rush can viably contend that there is some kind of legal gray area regarding whether *this* information "relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual," as long as it "identifies … or can be used to identify the individual." 42 U.S.C. § 1320d(6). It remains the case, however, that if Kurowski cannot carry her burden to show that Rush *in fact* collected her private, care-related information in addition to identifying information, then she will not prevail on her Wiretap Act claim for the reasons discussed in the Court's decisions dismissing previous versions of her claim. Similarly, if Rush in fact was unaware of the nature of the information that it was transmitting to Facebook, Google, and Bidtellect, then that potentially could be a defense not only to the Wiretap Act's requirement that it acted with *purpose* but also HIPAA's requirement that it acted *knowingly*.

In sum, the Court concludes that Kurowski has plausibly alleged that Rush acted with the conscious desire to knowingly make unauthorized disclosures of her IIHI to Facebook, Google, and Bidtellect for purposes of invoking the crime-or-tort exception. As a result, Rush is not entitled to judgment as a matter of law on her Wiretap Act claim.

4. Section 1292(b) certification

Rush asks the Court to certify the question of "whether plaintiffs can adequately state a Wiretap Act claim under the tortious or criminal conduct exception" to the Seventh Circuit for an interlocutory appeal under 28 U.S.C. § 1292(b). Section 1292(b) permits a court in a civil case to certify an otherwise non-appealable order for appeal if it

"involves a controlling question of law as to which there is substantial ground for difference of opinion and that an immediate appeal from the order may materially advance the ultimate termination of the litigation." As discussed, the Court acknowledges that there is no definitive Seventh Circuit guidance regarding the requirements of section 2511(2)(d) and the precise contours of HIPAA's application to tracking technologies. But an answer to Rush's question presented necessarily requires careful engagement with the specific facts alleged in this case. Although whether a plaintiff has stated a claim is a question of law, the Seventh Circuit has explained that section 1292(b) certification is appropriate for "abstract legal issue[s]," and not simply any "issue that might be free from a factual contest." *Ahrenholz v. Bd. of Trs. of Univ. of Ill.*, 219 F.3d 674, 677 (7th Cir. 2000). The question here is not "a pure question of law" that "the court of appeals could decide quickly and cleanly without having to study the record." *Id.* Moreover, as the Court has explained, Kurowski alleges that Rush *intentionally* programmed its web properties to intercept and transmit *specific* MyChart data that Rush *knew* was IIHI, such as her appointments with Rush physicians and information about her medical conditions. This is sufficient to plausibly allege that Rush was on notice that its conduct was illegal. Thus, even if the Seventh Circuit were to conclude that "purpose" under section 2511(2)(d) requires knowledge that the party's intended act is illegal, Kurowski's claims would survive. The Court therefore concludes that an immediate appeal is unlikely to "materially advance the ultimate termination of the litigation." 28 U.S.C. § 1292(b).

B. Breach of contract claim

Rush argues that it is entitled to judgment on Kurowski's breach-of-contract claim

because she has not plausibly alleged that she suffered actual damage as a result of Rush's alleged breach. Kurowski responds that she can state a claim for breach of contract because she is entitled to "nominal damages" even if the breach did not result in actual damage. The parties agree that Illinois law governs the breach of contract claim.

The Seventh Circuit has stated numerous times that "Illinois law is clear that, to state a claim for breach of contract, one must be able to prove actual damage." *TAS Distributing Co.*, 491 F.3d 625, 631 n.6 (7th Cir. 2007); *see also Gociman v. Loyola Univ. of Chic.*, 41 F.4th 873, 883 (7th Cir. 2022); *Spitz v. Proven Winners N. Am., LLC*, 759 F.3d 724, 730 (7th Cir. 2014); *Wigod v. Wells Fargo Bank, N.A.*, 673 F.3d 547, 560 (7th Cir. 2012); *Catalan v. GMAC Mortg. Corp.*, 629 F.3d 676, 694 (7th Cir. 2011); *Fednav Int'l Ltd. v. Cont'l Ins. Co.*, 624 F.3d 834, 839 (7th Cir. 2010). "Merely showing that a contract has been breached without demonstrating actual damage does not suffice, under Illinois law, to state a claim for breach of contract." *TAS Distributing Co.*, 491 F.3d at 631; *see also Prima Tek II, L.L.C. v. Klerk's Plastic Indus., B.V.*, 525 F.3d 533, 541 (7th Cir. 2008) (rejecting the plaintiff's argument that, under Illinois law, "it should have been awarded nominal damages if it could not prove actual damages"). Although the cases Kurowski cites suggest there is some inconsistency among Illinois courts on this question, this Court is bound by the Seventh Circuit's interpretation of Illinois law. *See Luna v. United States*, 454 F.3d 631, 636 (7th Cir. 2006) ("[T]he district court should not be making contrary predictions [about state law] when [the Seventh Circuit] has ruled squarely on the matter."). Kurowski therefore must plausibly plead that she has suffered actual damage from Rush's breach in order to state a claim.

As the Court has previously explained, Kurowski has not plausibly alleged that she suffered actual damage. *See Kurowski II*, 683 F. Supp. 3d at 845–47 (explaining why each of Kurowski's various theories of actual damage was insufficient). Although that order pertained to the allegations pleaded in Kurowski's first amended complaint, she has not pointed the Court to any new allegations in her second amended complaint that would warrant a different outcome on this issue. The Court therefore concludes that Rush is entitled to judgment on Kurowski's breach-of-contract claim because she has not plausibly pleaded that she suffered actual damage.

C. Illinois Eavesdropping Act claim

Rush argues that Kurowski's failure to plausibly plead actual damage likewise entitles it to judgment on her Illinois Eavesdropping Act claim. The Act provides the following remedies to injured parties:

> (a) To an injunction by the circuit court prohibiting further eavesdropping by the eavesdropper and by or on behalf of his principal, or either;
> (b) To all actual damages against the eavesdropper or his principal or both;
> (c) To any punitive damages which may be awarded by the court or by a jury.

720 ILCS 5/14-6. Rush argues that, under Illinois law, "the plaintiff can only be awarded punitive damages where actual damage is shown." Def.'s Mot. for J. on the Pleadings at 10 (quoting *Florsheim v. Travelers Indem. Co. of Ill.*, 75 Ill. App. 3d 298, 309–10 (1st Dist. 1979)). Rush therefore argues that Kurowski's "claim for punitive damages under the Illinois Eavesdropping Act also is dependent on [her] ability to state claim for actual damages under the statute." *Id.* at 11. Kurowski argues that (1) Illinois common law permits punitive damages in the absence of actual damages, and (2) regardless of the common law rule, the statute makes clear that "punitive damages" are available as a

"separate and independent category from 'actual damages.'" Pls.' Resp. at 13–14.

The Court first addresses the statutory argument. The Court agrees with Kurowski that, unlike some Illinois statutes, the Eavesdropping Act does not expressly require that a plaintiff show "actual damage" to seek recovery. *See, e.g.*, 815 ILCS 505/10a(a) ("Any person *who suffers actual damage* as a result of a violation of [the Illinois Consumer Fraud and Deceptive Business Practices Act] committed by any other person may bring an action against such person." (emphasis added)). Instead, the Act states that "*[a]ny or all parties* to any conversation or electronic communication upon which eavesdropping is practiced contrary to this Article *shall* be entitled" to the Act's civil remedies. 720 ILCS 5/14-6(1) (emphasis added).

Rush cites to the fact that the civil remedies section of the Act is entitled "Civil remedies to injured parties." *See* 720 ILCS 5/14-6. But a party can suffer an injury—such as a privacy violation—without suffering economic harm. *Cf. TransUnion LLC v. Ramirez*, 594 U.S. 413, 425 ("[I]njuries with a close relationship to harms traditionally recognized as providing a basis for lawsuits in American courts . . . include, for example, reputational harms, disclosure of private information, and intrusion upon seclusion."); *see also Rosenbach v. Six Flags Entertainment Corp.*, 2019 IL 123186, ¶ 25, 129 N.E. 1197, 1204 (2019) (rejecting the argument that the phrase "aggrieved person" in the Biometric Information Privacy Act "limit[s] a plaintiff's right to bring a cause of action to circumstances where he or she has sustained some actual damage" because "[w]hen the General Assembly has wanted to impose such a requirement in other situations, it has made that intention clear").

This does not mean, however, that Kurowski is automatically entitled to punitive

damages as long as she states a claim under the Act. In *McDonald's Corp. v. Levine*, 108 Ill. App. 3d 732, 738–39, 439 N.E.2d 475, 480 (1982), the court explained that "the three civil remedies" in the Act represent the "codification of the traditional common-law remedies afforded to anyone whose rights have been tortiously violated." The court therefore stated that "[a]lthough punitive and compensatory damages may be awarded by a court or jury . . . the victim must prove he is entitled to damages in the same manner as he would in any common law tort action." *Id.* at 739, 439 N.E.2d at 480; *see also By-Prod Corp. v. Armen-Berry Co.*, 668 F.2d 956, 961 (7th Cir. 1982) ("[T]he legislature presumably intended that the discretion of the court or jury [under the Eavesdropping Act] would be controlled by the general principles of Illinois law governing punitive damages."). Rush argues that, in Illinois, "the plaintiff can only be awarded punitive damages where actual damage is shown." Def.'s Mot. for J. on the Pleadings at 10 (quoting *Florsheim v. Travelers Indem. Co. of Ill.*, 75 Ill. App. 3d 298, 309–10).

The Seventh Circuit has recognized that, although there is support for this general rule, a different line of cases states that punitive damages may be awarded in cases "either where 'malice, violence, oppression or wanton recklessness, mingle in the controversy,' or where the act complained of partakes a criminal or wanton nature,'" even if the plaintiff did not suffer actual damage. *See By-Prod Corp.*, 668 F.2d at 962 (quoting *McNay v. Stratton*, 9 Ill. App. 215, 221 (1881)). More recent authority from Illinois courts likewise suggests that actual harm is not a prerequisite for an award of damages with respect to intentional torts. *See, e.g.*, *Kirkpatrick v. Strosberg*, 385 Ill. App. 3d 119, 133 (2008); *In re Est. of Hoellen*, 367 Ill. App. 3d 240, 253, 854 N.E.2d

774, 786 (2006) ("Our courts have determined that punitive damages are appropriate to punish and deter conduct where a defendant, as in this case, is found to have committed an intentional breach of fiduciary duty," even absent actual damage).

As discussed extensively with respect to the Wiretap Act claims, Kurowski alleges that Rush intentionally programmed its web properties to intercept and transmit patients' sensitive health data *specifically* even though it knew it was not authorized to do so. This conduct is therefore akin to an intentional tort, and a reasonable factfinder could conclude that it was "accompanied by aggravated circumstances such as wantonness, willfulness, malice, fraud, or oppression, or when the defendant acts with such gross negligence as to indicate a wanton disregard for the rights of others." *In re Est. of Hoellen*, 367 Ill. App. 3d at 253, 854 N.E.2d at 786. The Court therefore denies Rush's motion to dismiss Kurowski's claim under the Illinois Eavesdropping Act.

Conclusion

For the above reasons, the Court grants Rush's motion for judgment on the pleadings [dkt. no. 90] with respect to Kurowski's breach-of-contract claim but otherwise denies the motion. The Court denies Rush's motion to certify its Wiretap Act claim for an interlocutory appeal under 28 U.S.C. § 1292(b). The case is set for a telephonic status hearing on July 29, 2024 at 9:00 a.m., using call-in number 650-479-3207, access code 980-394-33. The parties are directed to file a joint status report on July 22, 2024.

Date: July 18, 2024

MATTHEW F. KENNELLY
United States District Judge